STRATEGY RESEARCH PROJECT

STRATEGIC INTELLIGENCE FOR TACTICAL OPERATIONS: INTELLIGENCE REQUIREMENTS FOR FORCE PROJECTION OPERATIONS

BY

COLONEL STEPHEN J. BOND
United States Army

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

Strategic Intelligence for Tactical Operations: Intelligence Requirements for Force Projection Operations

by

COL STEPHEN J. BOND
UNITED STATES ARMY

Col. Jay E. Lawson
Project Advisor

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

ABSTRACT

AUTHOR: Stephen J. Bond, COL, US Army

TITLE: Strategic Intelligence for Tactical Operations: Intelligence Requirements for Force Projection Operations

FORMAT: USAWC Strategy Research Project

DATE: 4 April 1998 **PAGES:** 47 **CLASSIFICATION:** UNCLASSIFIED

In the post-Cold War world, U.S. Armed Forces will conduct force projection operations more frequently to respond to crises. The military will place demanding requirements on the National Intelligence Community to provide intelligence to support contingency operations. Where do we need to focus for threats in the future? What are the Armed Forces' intelligence requirements to support force projection operations? This study argues that the National Intelligence Community must understand the information requirements of the Armed Forces and narrow their products to meet tactical commanders' needs when supporting crisis operations. It briefly discusses areas for future conflicts, highlights crisis and deployment operations, and provides a general statement of information requirements for these operations. It uses recent historical examples (such as Operation JUST CAUSE in Panama and Operation DESERT SHIELD in Saudi Arabia) to support its conclusions.

TABLE OF CONTENTS

INTRODUCTION

Since the end of the Cold War, the U.S. intelligence and defense communities have refocused to meet the changing strategic needs of our nation. These two communities share the strategic imperative to shape the national security environment, to respond to crises, and to prepare for tomorrow in support of our national strategy of engagement and enlargement.[1] Our national leaders rely on the Intelligence Community (IC) to provide warning of impending crises. This community also provides information for economic, diplomatic, political, informational, and military tools of power. The Armed Forces are frequently our leaders' instrument of choice for responding to many emerging threats.

When our national leaders call on the Armed Forces to respond, our national prestige is at stake. The response thus becomes a high-risk venture. Further, our strategy relies on force projection rather than forward presence.[2] The Armed Forces must therefore maintain a global orientation and deploy from the United States to respond to crises.[3] The Intelligence Community (IC) provides our national leaders with timely intelligence and identifies where future crises might occur. It

also provides information for the Armed Forces to respond effectively.

This study identifies the intelligence requirements of Armed Forces' commanders and units. It provides a strategic look at potential crises and formulates a tactical statement of information requirements for producers of intelligence. It offers a general statement of interest. It will thus assist strategic assets and analysts in understanding the information needs of the Armed Forces. This study does not replace the priority intelligence requirements of a Joint Forces Commander or requirements of an intelligence collection manager for a specific operation. Rather, it can serve as a primer for intelligence professionals receiving support and supporting military operations.

This study describes current trends in the Armed Forces and IC, identifies IC components and functions, and discusses future threats and potential crisis situations. It provides a brief explanation of Armed Forces doctrine for force projection, cites intelligence lessons from operational experiences in Panama and the Persian Gulf, and finally, it examines the basic information needed to support military operations.

TRENDS

> At the strategic level, [intelligence] was fine. But we did not get enough tactical intelligence -- front-line battle intelligence.
>
> Lieutenant General William M Keys, USMC
> Commanding General, 2nd Marine Division
> during Operation Desert Storm[4]

Force projection operations require joint forces to deploy from garrisons to a crisis location. To achieve success, the Armed Forces must leverage the capabilities and potential of the United States' Intelligence Community. General Keys notes the inability during Operation DESERT STORM of the IC to provide information with tactical resolution to deployed military forces. The solution to this requires more than providing a conduit to the intelligence agencies. Such access certainly helps, but it is not the entire answer. Members of the IC must understand military operations. Intelligence professionals must know what their customers need, then get this information to the customer. Similarly, members of the Armed Forces must know where to get information from the IC. There are other trends that will require the IC and Armed Forces to work closely in tandem to identify and resolve crises. These are:

- The frequency of crisis deployments for the Armed Forces has increased during the past ten years. This trend will continue. Additionally, the timelines for the Armed Forces to respond to crises will decrease in the future.

- National intelligence systems will be the first U.S. assets on the scene of a crisis, sometimes after the media has informed the world of the incident. The IC must provide warning, then rapidly disseminate information on the situation. The IC must continue this focus, even after theater and tactical intelligence elements are on site to perform collection and production of intelligence.

- Tactical intelligence systems will deploy from their home stations with their supported units. Military units will deploy with a "high tooth to tail ratio." Days, weeks, or sometimes months may go by before tactical intelligence assets are in position to collect and generate intelligence. However, the requirement for tactical resolution remains a necessity. Those organizations providing support must provide tactical fidelity for crisis resolution.

- Cracks between the tactical and strategic intelligence communities are likely to grow in the future. Intelligence personnel assignment policies will "track" military intelligence professionals into either strategic or tactical intelligence fields. Intelligence professionals working at the strategic level will increasingly have limited tactical experience.[5]

THE NATIONAL INTELLIGENCE COMMUNITY

> National-level intelligence agencies and organizations that can support military operations should make that support available. Additionally, they should assist in identifying other potential intelligence requirements that may be addressable through their capabilities.
>
> - Joint Pub 2-01[6]

The U.S. Intelligence Community comprises the intelligence organizations in the Executive Branch of government. The

Director of Central Intelligence (DCI) heads the IC. The DCI is the President's principal advisor on intelligence and heads the Central Intelligence Agency (CIA). Along with the CIA, other members of the community include:

- Department of Defense (DOD) intelligence elements, including Defense Intelligence Agency (DIA), National Security Agency (NSA), National Reconnaissance Office (NRO), National Imagery and Mapping Agency (NIMA), service (Army, Navy, Marine, Air Force) and unified command intelligence organizations. Obviously, DOD elements, along with the CIA, are most focused on the needs of the military.

- Intelligence elements of the Department of Justice, Department of the Treasury; Department of Energy; and Department of State. These elements are generally less focused on the Armed Forces' needs.[7]

All members of the National IC have the first priority of providing information to our national leaders. The collective community also performs the following functions:

- Provide indications and warning (I&W) of conflict and threats to U.S. interests;

- Monitor treaty compliance;

- Support negotiators;

- Provide economic and political developments and assessments;

- Provide information about emerging technology;

- Protect against hostile intelligence services and others seeking classified information;

- Provide support to anticipated or ongoing military operations.[8]

All these functions, to varying degrees, are of interest to and may directly support the Armed Forces. Of particular interest are the functions of providing warnings of conflict and supporting military operations.

One of the IC's major achievements in the post-Cold War years has been their refocused effort to meet the needs of the Armed Forces. In 1993, Vice President Al Gore's Committee on Reinventing Government identified the lack of support for military operations as an IC weakness.[9] The Committee charged the IC to "improve support to ground troops during combat operations." This initiative succeeded in shifting IC attitudes toward better supporting the military.

The IC has genuinely tried to improve support to the Armed Forces over the past ten years. However, there is still room for improvement. Surely, the IC-Military relationship must not be a "war marriage". It must begin before the Armed Forces are in combat and should not end when they have completed operations. This relationship will not happen "naturally". Indeed the IC has gone to great lengths to educate military tacticians on available strategic intelligence platforms,

systems, agencies, and products. The CIA's office for military support and coordination is one example of efforts to improve support.[10] Another is the Joint Staff J2 and DIA's deployable National Intelligence Support Teams, created to provide linkage and liaison from CIA, NSA, and DIA to the deployed force.[11]

Today, the collective IC cites support to the military commander or "Warfighter" as one of its core tasks.[12] However, in crisis deployments, intelligence to support the tactical "warriors" is drawn from strategic intelligence assets. This is different from the "Warfighter". The information needs of battalions, squadrons, task groups, brigades or Joint Task Forces differ greatly from the needs of the warfighting theater commander. Tactical support requires a thorough understanding of tactical requirements.

Information technology has enabled an information conduit from national agencies and collectors to the tactical level. Deployed Brigade-, Squadron- and Battalion-level elements will soon be able to read intelligence reports from CIA or see the latest satellite images in real time.[13] However, military tacticians need more than a conduit for the latest intelligence reports. Military planners will find little relevance in reports posted for Washington policymakers. Crisis support

requires strategic assets and agencies to be front-loaded, updating the right databases, and providing relevant information and answers, even before questions are asked. To conduct a "brilliant push" of information over the information circuits, they must provide the tactical resolution needed to conduct military operations. Otherwise, we have not leveraged our technological advantage.

Providing intelligence support for tactical units is an enormous undertaking. Current discussions between the IC and the Armed Forces focus on the structure of the IC and the products they provide.[14] Structure, organization, and linkages are also the major topics in Armed Forces doctrine.[15] The tone of the dialogue is largely informational and educational. This proliferates into Armed Forces doctrine.[16] What we lack is a statement of the information needed by the Armed Forces.[17] We have outlined the structure and process of linking systems, while neglecting the most important piece of our business--the quality and timeliness of the information. We assume that by connecting military customers to the intelligence agencies, somehow the right information will flow. This is an oversimplification and a large assumption. What makes all intelligence professionals useful and relevant is the quality of

collected and processed information.[18] The IC must understand and deliver what their military customers need. This can be achieved through the study of military doctrine, tactics and techniques. It can also occur through National Agency participation in military exercises and analyst-to-analyst exchanges with tactical elements (below CINC level). Without such study and experience, how can an intelligence analyst, working in a national agency or even a theater Joint Intelligence Center, actually know what information military units require? The time has come to open the dialogue on this void. The starting point is identifying potential crisis areas.

THE CURRENT ENVIRONMENT AND FUTURE THREATS

> The cold war is over, but many new dangers have taken its place: Regional security threats; the proliferation of weapons of mass destruction; terrorists who, as we have seen, can strike at the very heart of our major cities; drug trafficking and international crime.
>
> - William J. Clinton (1995)[19]

It has become a cliché to say that the post-Cold War era is a complex period of uncertainty and turmoil. The rise of a peer competitor like the former Soviet Union is unlikely for at least 15 years.[20] Gone is the lately perceived "comfort" of a defined enemy. Indeed we face a variety of threats today. Threats and challenges of the future will require our Armed Forces to

prepare for unanticipated and unpredictable events, asymmetrical challenges, regional instability, and transnational threats.[21]

Our national leaders will call on the Armed Forces to respond to a variety of situations across the range of military operations. These operations will range from war, to lesser conflicts, and to peacetime engagements. The types of operations will vary from major theater war to the smallest of small-scale contingencies.[22] Peacetime operations for the Armed Forces have increased dramatically over the past ten years. Our military has engaged in such diverse activities as security assistance; search and rescue; noncombatant evacuations; peacekeeping; peacemaking; shows of force; countering terrorism, proliferation of weapons of mass destruction, and drugs; humanitarian assistance; and disaster relief.[23] All of these activities require significant intelligence support.

The IC must focus on developing situations and building hot spots for future crises. Threats that could potentially challenge our interests and require a response from the Armed Forces include:

- A resurgent, hostile major power such as Russia or China.
- Major theater conflict with Iran, Iraq, North Korea, or other unforeseen hostile regional powers or coalitions.
- Peacekeeping, peace enforcement, or conflicts with failing states or involving the internal strife of ethnic,

national, religious or tribal groups. This strife will threaten lives, force migration, and undermine stability of the region. States in the former Yugoslavia, many African countries (Somalia, Rwanda, Burundi, Liberia, Zaire, Congo, etc.), some former Soviet Republics, Colombia, Cambodia, North Korea, and Cuba currently fall into this category.

- Efforts to deny or preempt rogue states (Iran, Iraq, Libya, North Korea, Syria, etc.) from obtaining weapons of mass destruction and missile delivery technology.

- Action against state or transnational sponsors of international terrorism, illegal drugs, and crime.

- Efforts to prevent subversion, lawlessness, and other threats to democracies and reform, such as in the former Soviet Union, East Europe, Latin America, etc.

- Humanitarian and disaster relief operations.

- Other threats against U.S. prosperity and economic growth.[24]

CRISIS ACTION PLANNING AND FORCE PROJECTION DOCTRINE

> Commanders, in turn, must strive to articulate how national intelligence can serve their tactical needs.[25]

Our Armed Forces prepare for crisis operations when incidents occur which involve threats to United States' interests. These may be threats to our territory, citizens, forces, or other interests that create conditions of diplomatic, political, economic, or military importance.[26] Success in future crisis operations will depend on two things--the accuracy and speed of relevant information, and the speed and mobility of the

deploying units. To plan and conduct operations, deploying forces must have a detailed understanding of the situation. National and theater intelligence assets and agencies play a pivotal role in this from the initial crisis warning to providing information to resolve the situation.

Our National Command Authorities, the Joint Staff, the Regional CINCs, their staffs, and units conduct crisis planning using available information from the IC. There is no timeline for crisis planning, which the Joint Military Doctrine breaks into seven phases. These phases may last hours to months. Some may be compressed or eliminated, depending on the nature of the crisis.[27]

- Phase I - Situation Development: After receiving initial reports on a crisis, national and theater intelligence assets shift to monitor and assess the implications of the crisis.

- Phase II - Crisis Assessment: The Department of State, the IC, and DOD (including the Regional Commander-in-Chief and staff) focus on the situation and increase crisis reporting.

- Phases III, IV, and V - Developing Military Courses of Action, Selecting the Course of Action, and Planning the Execution. All three phases require extensive intelligence support. Intelligence assets track the situation. Analysts

provide background information and future assessments for planners and units preparing for deployment. In these planning phases, reserve components are mobilized. Units plan and prepare for deployment. For smaller scale contingencies, the Regional CINC may assemble a subordinate Joint Task Force to respond to the crisis. Continuity of intelligence during the crisis is imperative as this task force assembles, plans, and prepares to conduct operations.

- Phase VI - Execution: Units deploy into the crisis area. National and theater intelligence assets and agencies provide tactical coverage as deploying intelligence elements enter the crisis area. Forces enter the crisis area by forcible entry or permissively through a friendly port of entry.

The salient characteristics of force projection operations are an early response with a rapid projection of military power.[28] The Armed Forces will attempt to resolve the situation quickly and with minimum casualties. Forcible entry into the objective area could occur by parachute, by helicopter, or by amphibious assaults (as occurred in JUST CAUSE in Panama and RESTORE HOPE in Somalia). Successful forcible entry operations require:

- Detailed intelligence and unity of effort.

- Forces prepared to fight upon arrival, supported by robust command, control, communications, computer, and intelligence (C4I) capabilities to move with forward elements.

- Operations security and deception.

- Speed and surprise.

- Preparatory support from Special Operations Forces.[29]

A build-up and staging of combat forces through friendly ports could also occur (as in Saudi Arabia during DESERT SHIELD). After a rapid build-up of forces, decisive operations begin.

When tactical intelligence assets arrive and begin operations in the crisis area, an intelligence crossover point occurs. At this point, the units conducting operations will rely more on tactical intelligence collectors than on strategic and theater intelligence assets. Before this point, strategic and theater collectors and analysts must set the conditions for the Armed Forces success.

Intelligence staffs and deploying units perform the following tactical intelligence functions: indications and warning; situation development; target development; battle damage assessment; intelligence preparation of battlefield; force protection and counterintelligence operations; and collecting, managing, and disseminating intelligence.

- Phase VI is the redeployment of forces. Finally, Phase VII calls for demobilization of reserve forces. Once the deployed forces accomplish the assigned objectives, they conduct conflict termination operations. Then they redeploy, reconstitute the forces, and demobilize. As tactical intelligence elements leave the theater, redeploying units once again rely on national and theater intelligence assets to monitor the situation and support security force protection operations.

FORCE PROJECTION CASE STUDIES AND INTELLIGENCE LESSONS LEARNED

The force projection case studies of Panama (1989) and the Persian Gulf (1990) provide examples of the types of crisis operations the Armed Forces will perform in the future. The following historical vignettes will briefly describe the operations and discuss intelligence lessons learned. These force projection operations provide valuable lessons regarding intelligence support for future military operations.

OPERATION JUST CAUSE--PANAMA 1989-1990

JUST CAUSE was small-scale contingency operation conducted in Panama beginning in December 1989. Its purpose was to create a safe environment for U.S. citizens living in Panama; ensure the integrity of the Panama Canal and other key sites; provide a

stable environment for the freely elected government of Panama; and to apprehend Panamanian dictator and indicted drug trafficker, Manuel Noriega.[30] As a force projection operation, JUST CAUSE was unique in that the U.S. Armed Forces had a robust presence in Panama. Roughly half of the 27,000 forces used in the operation were in Panama before hostilities began.[31]

Planning for the operation began in 1988; however, final planning and designation of a Joint Task Force to conduct the operation did not occur until August 1989.[32] On December 19, 1989, U.S. military forces deployed from U.S. bases in the United States and Panama to strike or secure 26 separate locations in Panama. The effect of these simultaneous strikes broke the back of the Panamanian Defense and Police Forces (PDF) and chased Manuel Noriega into hiding.

The post-invasion investigation conducted by the House Armed Services Committee (HASC) concluded this was a highly successful operation. The HASC reported there were no significant intelligence "failures."[33] However, they expressed concern over the adequacy of HUMINT and its integration into military planning.[34] The HASC found military planners underestimated the resistance of the PDF and (especially) the paramilitary Dignity Battalions. The biggest "surprise" was the

80,000 weapons Noriega had cached throughout the country, and their intended use. Many believe Noriega intended to sell these arms to insurgents, terrorists, or drug lords.[35]

Other "mistakes" mentioned by the HASC included the U.S. inability to track and capture Noriega, and the failure to anticipate his run to the Papal Nunciate.[36] Before the operation, SOUTHCOM was attempting to track Noriega and claimed to know where he was 75 to 80 percent of the time.[37] As events would prove, this information was not sufficient to apprehend him.

The HASC mentioned the unexpected appearance of armored cars at one of the objectives, Paitilla Airport. This resulted in the death of four Navy SEALS. The HASC determined this incident was a risk associated with any military operation; thus was not a "failure" of intelligence. However, the requirement to track individual armored cars identifies an excellent point on the level of detail needed to support contingency operations.

Despite our long established presence in Panama, HUMINT was the major intelligence weakness. The Army Center for Lessons Learned makes an interesting observation on HUMINT for JUST CAUSE. The report states HUMINT provided invaluable information through the pre-deployment phase of JUST CAUSE, even though

HUMINT collection units were restricted by national policy and lacked personnel to accomplish the task.[38] Yet the conditions for HUMINT are likely never to be better. Generally target information, gathered from all sources of intelligence, was outstanding. What was lacking was information on Noriega and PDF intentions before and after the operation began. This lesson shows the difficulty of establishing HUMINT, even in countries where we have an established presence. Additionally, with months to prepare, neither the national agencies nor USSOUTHCOM produced a "BLACK-WHITE-GRAY" list. The BLACK-WHITE-GRAY list is a database which compiles and classifies known hostile, friendly, and other persons of interest in the crisis area. Instead the Joint Task Force produced its own "Most Wanted List" to ferret out Noriega accomplices after the operation was underway.[39]

OPERATION DESERT SHIELD--PERSIAN GULF 1990-1991

Operation DESERT SHIELD was the U.S. and U.N. Coalition response to Saddam Hussein's invasion of Kuwait on August 2, 1990. It unfolded beginning in July when Saddam accused Kuwait and the United Arab Emirates of conspiring with the U.S. to drive down oil prices, thereby stealing billions of dollars from Iraq. The IC played a key role in providing the warning of

Saddam Hussein's build-up of forces along the Kuwait border and his subsequent invasion. By the end of July, they reported five of Saddam Hussein's finest divisions, over 100,000 troops, were in Southern Iraq near the Kuwaiti border. On August 1, CIA, DIA, and CENTCOM issued warnings of an Iraqi invasion into Kuwait.[40] However, most senior leaders in the United States, as well as allied countries, did not believe the early IC warnings.[41] Following their attack into Kuwait, it appeared the Iraqi forces were preparing to attack into Saudi Arabia. CENTCOM alerted its forces in response.

On August 6, President Bush authorized U.S. air, naval, and ground forces to deploy to the Persian Gulf.[42] Their objectives were to seek the "immediate, unconditional and complete withdrawal" of Iraqi forces from Kuwait and to defend themselves and Saudi Arabia from further Iraqi aggression.[43]

There were several intelligence lessons learned from this operation. On the positive side, Gen. Colin Powell, Chairman of the Joint Chiefs of Staff, stated "Intelligence support to Operation Desert Shield and Desert Storm was a success story."[44] However, there were also comments like those from General Keys about the lack of information to support tactical operations.

The IC produced numerous reports and special products including fact books, "how-they-fight" manuals, and targeting templates. All of these were generally good. However, despite the fact that nearly all the U.S. intelligence capabilities were focused on this crisis, division, brigade, and wing commanders were universally frustrated and dissatisfied with the intelligence support they received.[45] Their most common complaint was the products lacked details needed to plan and conduct tactical operations. Even so, most units were grateful for the intelligence received from national intelligence assets.[46] In many cases this was the only intelligence received. Some tactical intelligence systems were not allowed to collect information. Others were not optimally sited. These restrictions resulted from operations security precautions before the offensive phase of the operation.[47] Consequently, tactical commanders' intelligence requirements were passed to higher echelons and tactical units relied on reports from national and theater intelligence centers. Tactical requests were assigned a relatively low priority, as theater and national assets were already heavily tasked.[48] Using "vague" reports, units attempted to provide tactical relevance.[49]

There was an insatiable desire for imagery.[50] The requirement for more tactical reconnaissance and imagery was not met in the eyes of the tactical commanders.[51] One Division G2 said he could get imagery, but not of his division's specific objectives.[52] While national and theater assets collected imagery, getting it to the tactical commanders was not easy. Many imagery dissemination systems were deployed. However, these could not accommodate the massive requirements through limited communication circuits. To meet hard copy imagery requirements, couriers delivered large quantities of imagery to tactical units.[53]

Other factors contributed to tactical commanders' complaints. The intelligence agencies, including DIA and CIA, employed the concept of "competing analysis". This gave consumers of intelligence products the benefits of alternative views.[54] Field commanders criticized these divergent products as being too broad and non-predictive. They charged the products were appropriate for policymakers but not relevant to a combat commander.[55]

Another contributor to the problem was the blurring of tactical collectors and strategic assets. For example, standoff theater collectors such as Joint STARS were used for hunting

SCUD missiles. To fill the gap this created in theater coverage, the Army's tactical OV-1D Mohawk's side looking airborne radar was used.

After the initial Iraqi SCUD firings, hunting the mobile SCUD launchers took on a new importance. Finding the mobile launchers became a major task for the military and the IC. This task directly competed with requirements of the tactical commanders, straining collectors as the coalition was planning and conducting offensive operations. Hunting mobile SCUD launchers and post-strike assessments posed major challenges as the military began offensive operations in January through the conclusion of hostilities in February 1991.

INTELLIGENCE REQUIREMENTS TO SUPPORT MILITARY OPERATIONS

The primary objective of intelligence support to military operations is providing commanders with timely, complete, and accurate understanding of the battlespace (operating environment), and of the adversary.[56] Intelligence staffs and units fuse all sources of information and intelligence to provide the commander with useful information and reduce uncertainty. This enables the commander to anticipate the battle and influence the outcome of operations.[57] For contingency operations in war or military operations in other than war, basic structure and

information requirements are similar.[58] However, operations other than war and small-scale contingency operations require even more detailed threat information. To reduce U.S. casualties, military commanders often want finite information on potential threats, which may include small units (squad or police patrol level) or individual armored vehicles.

Before a deployment, commanders urgently need intelligence to develop courses of action and determine where to employ forces to achieve success.[59] Knowledge of the battlespace and information on the threat drives all the operating systems, which include maneuver; fire; information operations; reconnaissance, surveillance, and intelligence; air defense; and mobility and survivability. Intelligence also supports the integration of command and control and combat service support systems. The general intelligence information requirements for virtually all crisis operations include the following:

- An appreciation of the terrain and battlespace. This includes relief, hydrographic, cultural, and demographic information. It also includes climate and effects of weather on the battlespace.

- An understanding of the enemy. Of primary importance is information on his ground, air, air defense, and naval forces. Frequently, we also need information about the enemy's security and police forces. We need to know how he has organized and deployed. Additionally we need information on his intelligence,

surveillance, and reconnaissance capability for detecting our moves and positioning. Information on the enemy's level of training, leadership, morale, equipment, and will to fight is also needed.

- An understanding of what course of action the enemy is likely to follow: We also need to identify his strategic, operational, and tactical objectives and goals.

- Determining the enemy centers of gravity (strengths), and identifying his vulnerabilities and weaknesses.

- Identifying key nodes and links as potential targets: Key nodes and links include command, control, and computers (C3); power; transportation hubs and networks; military and government facilities; and air defense and early warning systems.

- Intelligence for supporting our information operations. This includes support for psychological operations, electronic attack, deception planning and operations, and operations security.

- Information on enemy intentions and capabilities to conduct operations and attacks against our forces in rear areas.

- Detecting enemy deceptions.

- Tracking the developing situation and providing a current operating picture of the battlefield.

- Identification of and specific information on landing areas for friendly and enemy airborne, heliborne, or amphibious forces.

- Locations of basic infrastructure, including heavy equipment for construction and material handling equipment, construction materials, and storage facilities: We should also know locations of sources of water, food, and other resources;

information on sea and air port facilities; and locations of medical facilities and supplies. We also need information on industries and facilities to assist service support planners and logistics elements.

Once operations begin, commanders need all the information mentioned above, along with updates on the tactical situation, emerging targets, and battle damage assessments.

All intelligence sources provide various pieces for the analytical puzzle. The intelligence disciplines (including Human-Source Intelligence, Signals Intelligence, Imagery Intelligence and Mapping, and Counterintelligence) provide information collectively, and with proper analysis, support the military operation.

HUMAN-SOURCE INTELLIGENCE (HUMINT)

HUMINT, the information derived from clandestine and overt human sources, is currently the weakest link in our capability to support military operations. HUMINT provides information on the adversary's intentions and other information extremely difficult to acquire by more technical collection means.[60] HUMINT received short shrift in the Cold War years, when more technical means of collection were favored. This is partially due to our national aversion to dealing with unsavory characters who may have a price for information and by our faith in

technology to provide solutions to hard problems. Consequently, we do not have agents in many volatile areas. This shortfall came to the forefront with our failures to capture Manuel Noriega in Panama in 1989; to find Aideed in Somalia in 1993; or to determine the maturity of the Iraqi weapons of mass destruction program. The creation of Defense HUMINT Services under DIA is an attempt to energize HUMINT support to the military.[61]

We cannot expect productive HUMINT operations to begin when a situation explodes into a crisis. Overt HUMINT collection could be restricted once a crisis occurs. Further, clandestine human sources must be developed over time. HUMINT assets may not be available to support military operations in difficult or denied target areas such as North Korea, Iran, or Iraq. Drug cartels, terrorist organizations, and international criminal organizations are even harder targets to penetrate.[62] Exposed agents are at best useless and at worst killed.

Many of our allies and coalition partners have robust HUMINT capabilities. One way to improve and obtain better, more responsive HUMINT is to trade our technically acquired imagery or SIGINT for HUMINT from our friends and partners.[63]

If a national agency has a well-placed source with key insights into the intentions of the enemy force, military commanders certainly need that information. However, during the early stages of a crisis, HUMINT needs may be as basic as having intelligence officers and commanders from deploying units talk with travelers familiar with the crisis area.

SIGNALS INTELLIGENCE (SIGINT)

The capability to collect SIGINT, or the information derived from intercepted communications, radar, and telemetry, is clearly a U.S. strength. SIGINT provides a major piece to the puzzle of enemy composition, disposition, location, intentions, and reactions. It provides early warning of hostile attacks and incoming ballistic missiles. We can lay out enemy air defenses and early warning radar through electronic intelligence and determine how best to avoid or defeat them. SIGINT also supports our information operations and assesses the effects of enemy information operations against us.

As with HUMINT, future crises are likely to occur in areas where we have limited data to support operations. Further, the collection of communications may not be continuous or constant in the early phase of a crisis. The deployed force intelligence officer must know how much collection coverage is available. He

must also know the times when there is limited or no SIGINT coverage.

IMAGERY INTELLIGENCE (IMINT)

IMINT and map products provide an appreciation of the terrain and show current enemy dispositions. This is clearly another U.S. strength. The military uses imagery to plan moves and to determine how the enemy will move against us. We use it to locate and update the enemy situation, and confirm enemy dispositions. We also use it to select targets, and to find and assess enemy obstacles. Through imagery, we initially select amphibious, airborne, and helicopter landing areas. We assess our attacks with post-strike imagery.

Overall, imagery products assist in planning our operations. They provide a picture of the battlefield. Military commanders want to see large, hard copy prints, even as the IC is switching to soft copy, computerized images. Military commanders really believe "a picture is worth a thousand words."[64] However, the latest available image is not always needed to answer most questions. Often, good quality, historical images will satisfy their needs.

COUNTERINTELLIGENCE (CI)

CI is information gathered and activities conducted to protect our forces against espionage, other intelligence activities, sabotage, or assassinations conducted on behalf of foreign powers, organizations, persons, or terrorists. Effective counterintelligence is critical to the security of operational forces. In most crisis deployments, the protection of forces is paramount. Once CI specialists arrive in the crisis area with the deployed forces, they provide antiterrorism and counterespionage services. Until these tactical assets arrive, U.S. forces must rely on national or theater HUMINT, SIGINT, IMINT, or host country assets. A major requirement for the Intelligence Community is to provide timely warning of possible terrorist attacks against our forces. Further, CI provides information on threat collection capabilities and activities. While CI was traditionally a human-source discipline, all sources of intelligence should be employed in the counterintelligence effort. Examples of this multi-disciplinary approach are monitoring our communications and viewing our positions using commercially available imagery. This helps determine what the threat can hear and see of our deployed posture.

One area of counterintelligence support that needs IC attention is the Black-White-Gray list. This database should be produced by national or theater agencies. However, in recent contingency operations the deploying task forces had to produce their own lists.

CONCLUSIONS AND RECOMMENDATIONS

In conclusion, the intelligence and defense communities must prepare now to meet the challenges of tomorrow. Currently there are many flash points, hot spots, and threats to our national interests. These threats require attention from the IC. This includes providing early warning and building intelligence databases for potential crisis areas. The Armed Forces should use this information to develop force structure, contingency plans, and capabilities to rapidly respond to crises.

When crises develop, the Armed Forces depend upon the IC to provide detailed tactical information for planning and conducting operations. The information required will range from peacetime intelligence and warnings to information needed by tactical commanders to conduct operations. In crisis operations, military forces rely on information from strategic and theater intelligence assets to see and hear the tactical

battlefield. Strategic collectors and analysts must know the basic information requirements of tactical commanders and units as they plan, prepare, conduct, and terminate operations.

Once a crisis occurs, we cannot rely on the IC and the operational forces to develop a working relationship. Thinking analysts must quickly provide information with tactical resolution and relevance. Analysts from the strategic to tactical levels must develop working relationships before a crisis. Through information technology, we have linkage from the tactical to strategic levels. Initiatives such as the national agencies' establishment of offices to support military operations and the deploying National Intelligence Support Teams are inherently good. However, <u>all</u> potential producers of intelligence must understand the needs of military consumers.

We must incorporate the lessons learned from previous operations to ensure we do not repeat the problems of the past. One of the primary lessons is that intelligence from strategic assets has lacked the required specificity to support tactical operations. We must overcome this. There must be a clear understanding of the Armed Forces basic information requirements to support operations ranging from major theater war to small-scale contingencies and peacetime operations. Finally, we have

lacked HUMINT to support crisis operations. The formation of the Defense HUMINT Services addresses this inadequacy. However, barring a turnabout in our national attitudes, this may not be enough. One solution is to have our allies and partners provide this type of information in exchange for our more technical intelligence.

With our national interests and prestige at stake, we must act now in anticipation of the next crisis requiring the deployment of military forces.

Word Count: 5,923

ENDNOTES

[1]William T. Clinton, A National Security Strategy for a New Century (Wash D.C.: The White House, 1997), 6-13.

[2]Department of the Army, Knowledge & Speed: The Annual Report on the Army After Next Project to the Chief of Staff of the Army (Wash, D.C.: U.S. Department of the Army, July 1997), 15.

[3]Department of Defense, National Military Strategy of the United States of America: Shape, respond, prepare now (Wash, D.C.: Joint Staff, September 1997), 15.

[4]Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress (Wash, D.C.: U.S. Government Printing Office, April 1992), 333.

[5]John M. Custer, "The Impact of OPMS XXI on MI Officers". Military Intelligence, 23, no. 4 (Oct-Dec 1997), 29.

[6]Department of Defense, Joint Intelligence Support to Military Operations, Joint Publication 2-01 (Wash, D.C.: Joint Staff, November 1996), x.

[7]John Deutch, A Consumer's Guide to Intelligence (Wash, D.C.: Office of Public Affairs, Central Intelligence Agency, 1995), 9-13.

[8]Hans Binnendijk, ed., Strategic Assessment 1996 (Wash, DC: National Defense University, 1996), 62.

[9]Al Gore, Creating a Government that Works Better & Costs Less: The Gore Report on Reinventing Government (New York: Random House, 1993), 94.

[10]Department of Defense, National Intelligence Support to Joint Operations (Final Coord. Draft), Joint Publication 2-02 (Wash, D.C.: Joint Staff, May 1995), B-1.

[11]Ibid., C-1.

[12]Jeffrey Richelson, The U.S. Intelligence Community, Third Edition (Boulder Colorado: Westview Press, 1995), 474. See also Binnendijk, ed., 68.

[13]William S. Cohen, Report of the Quadrennial Defense Review (Wash, D.C.: Department of Defense, 1997), 17. See also Binnendijk, ed., 69.

[14]Department of Defense, National Intelligence Support to Joint Operations (Final Coord. Draft), Joint Publication 2-02, chapters 1 & 2. See also Deutch, sections III & IV.

[15]Ibid.

[16]See Department of Defense, Joint Publications 2-0, 2-01, and 2-02.

[17]Binnendijk, ed., 69.

[18]Department of Defense, Joint Doctrine for Intelligence Support to Operations, Joint Publication 2-0 (Wash, D.C.: Joint Staff, May 1995), gl-8.

[19]"Our First Line of Defense": Presidential Reflections on US Intelligence (Wash, D.C.: Center for the Study of Intelligence, 1996), 56.

[20]Patrick M. Hughes, Global Threats to the United States and its interests abroad: Statement for the Senate Select Committee on Intelligence (Wash., D.C.: Defense Intelligence Agency (DIA), 1997), 2.

[21]Ibid., 9.

[22]Cohen, 17.

[23]Department of the Army, Decisive Force: The Army in Theater Operations, Field Manual 100-7 (Wash, D.C.: U.S. Department of the Army, May 1995), 8-8 to 8-10.

[24]William S. Cohen, Annual Report to the President and Congress (Wash, D.C.: U.S. Government Printing Office, 1997), 2.

[25]Binnendijk, ed., 69.

[26]Department of Defense, Doctrine for Planning Joint Operations, Joint Publication 5-0 (Wash, D.C.: Joint Staff, April 1995), III-9.

[27]Department of Defense, Doctrine for Planning Joint Operations, Joint Publication 5-0 (Wash, D.C.: Joint Staff, April 1995), III-11.

[28] Department of the Army, Decisive Force: The Army in Theater Operations, Field Manual 100-7 (Wash, D.C.: U.S. Department of the Army, May 1995), 6-3)

[29]Department of Defense, Joint Task Force Planning Guidance & Procedures (2nd Draft), Joint Publication 5-00.2 (Wash, D.C.: Joint Staff, July 1997), VII-17.

[30]Les Aspin, "Operation Just Cause: Lessons and Warnings in the Future use of Military Force" (Wash, D.C.: House Armed Service Committee Report, 1991), in Case Study: Operation Just Cause Panama 1989 (U.S. Army War College, Carlisle Barracks, Pa. 1994), 36.

[31]Ibid., 37.

[32]Bob Woodward, The Commanders (New York: Simon & Schuster, 1991), 100.

[33]Aspin, 40.

[34]Ibid.

[35]Ibid.

[36]Ibid.

[37]Ibid, 39.

[38]Center for Army Lessons Learned, Operation Just Cause Lessons Learned: Volume III, Intelligence, Logistics & Equipment (Fort Leavenworth, KS: U.S. Army Combined Arms Center, 1990), III-6.

[39]Ibid., III-10.

[40]Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress (Wash, D.C.: U.S. Government Printing Office, April 1992), 334.

[41]Woodward, 222.

[42]Ibid., 273.

[43]Ibid., 277.

[44]Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress, 333.

[45]Ibid., 340.

[46]Richard J. Quirk III, Intelligence for the Division -- A G2 Perspective (Carlisle, PA: U.S. Army War College, 1992), 142.

[47]Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress, 340.

[48]Ibid.

[49]Ibid., 342.

[50]Ibid., 338.

[51]Ibid., xviii.

[52]Quirk, 146.

[53]Department of Defense, Conduct of the Persian Gulf War: Final Report to Congress, 339.

[54]Ibid., 336.

[55]Ibid., 336-337.

[56]Department of Defense, Joint Intelligence Support to Military Operations, Joint Publication 2-01 (Wash, D.C.: Joint Staff, November 1996), I-1.

[57]Ibid., I-3.

[58]Department of Defense, Joint Doctrine for Intelligence Support to Operations, Joint Publication 2-0, VI-4.

[59]Department of the Army, Operations, Field Manual 100-5 (Wash, D.C.: U.S. Department of the Army, June 1993), 3-5.

[60]Richelson, 470.

[61]Deutch, 3.

[62]Richelson, 470.

[63]Harold Brown, Warren B. Rudman, et al., Preparing for the 21st Century: An Appraisal of U.S. Intelligence (Wash, D.C.: U.S. Government Printing Office, 1996, xxv.

[64]Quirk, 143.

BIBLIOGRAPHY

Aspin, Les. "Operation Just Cause: Lessons and Warnings in the Future use of Military Force". Wash, D.C.: House Armed Service Committee Report, 1991. In Case Study: Operation Just Cause Panama 1989. U.S. Army War College, Carlisle Barracks, Pa. 1994.

Binnendijk, Hans, ed. Strategic Assessment 1996. Wash, D.C.: National Defense University, 1996.

Brown, Harold; Warren B. Rudman; et al. Preparing for the 21st Century: An Appraisal of U.S. Intelligence. Wash, D.C.: U.S. Government Printing Office, 1996.

Center for Army Lessons Learned. Operation Just Cause Lessons Learned: Volume III, Intelligence, Logistics & Equipment. Fort Leavenworth, KS: U.S. Army Combined Arms Center, 1990.

Clinton, William T. A National Security Strategy for a New Century. Wash D.C.: The White House, 1997.

Cohen, William S. Annual Report to the President and Congress. Wash, D.C.: U.S. Government Printing Office, 1997.

Cohen, William S. Report of the Quadrennial Defense Review. Wash, D.C.: Department of Defense, 1997.

Custer, John M. "The Impact of OPMS XXI on MI Officers." Military Intelligence 23, no. 4 (Oct-Dec 1997): 29.

Department of the Army. Decisive Force: The Army in Theater Operations, Field Manual 100-7. Wash, D.C.: U.S. Department of the Army, May 1995.

Department of the Army. Intelligence and Electronic Warfare Operations, Field Manual 34-1. Wash, D.C.: U.S. Department of the Army, September 1994.

Department of the Army. Knowledge & Speed: The Annual Report on the Army After Next Project to the Chief of Staff of the Army. Wash, D.C.: U.S. Department of the Army, July 1997.

Department of the Army. Operations, Field Manual 100-5. Wash, D.C.: U.S. Department of the Army, June 1993.

Department of Defense. Conduct of the Persian Gulf War: Final Report to Congress. Wash, D.C.: U.S. Government Printing Office, April 1992.

Department of Defense. Doctrine for Joint Operations, Joint Publication 3-0. Wash, D.C.: Joint Staff, February 1995.

Department of Defense. Doctrine for Planning Joint Operations, Joint Publication 5-0. Wash, D.C.: Joint Staff, April 1995.

Department of Defense. Joint Doctrine for Intelligence Support to Operations, Joint Publication 2-0. Wash, D.C.: Joint Staff, May 1995.

Department of Defense. Joint Intelligence Support to Military Operations, Joint Publication 2-01. Wash, D.C.: Joint Staff, November 1996.

Department of Defense. Joint Task Force Planning Guidance & Procedures (2nd Draft), Joint Publication 5-00.2. Wash, D.C.: Joint Staff, July 1997.

Department of Defense. National Intelligence Support to Joint Operations (Final Coord. Draft), Joint Publication 2-02. Wash, D.C.: Joint Staff, May 1995.

Department of Defense. National Military Strategy of the United States of America: Shape, respond, prepare now. Wash, D.C.: Joint Staff, September 1997.

Deutch, John. A Consumer's Guide to Intelligence. Wash, D.C.: Office of Public Affairs, Central Intelligence Agency, 1995.

Gore, Al. Creating a Government that Works Better & Costs Less: The Gore Report on Reinventing Government. New York: Random House, 1993.

Hughes, Patrick M. Global Threats to the United States and its interests abroad: Statement for the Senate Select Committee on Intelligence. Wash., D.C.: Defense Intelligence Agency (DIA), 1997.

"Our First Line of Defense": Presidential Reflections on US Intelligence. Wash, D.C.: Center for the Study of Intelligence, 1996.

Quirk, Richard J. III. Intelligence for the Division--A G2 Perspective. Carlisle, PA: U.S. Army War College, 1992.

Richelson, Jeffrey. The U.S. Intelligence Community, Third Edition. Boulder Colorado: Westview Press, 1995.

Woodward, Bob. The Commanders. New York: Simon & Schuster, 1991.